

A REFERENCE FOR ORGANIZATIONS

Tips for spotting deepfakes

What to check in the image, the voice and the conversation, and which procedures protect the organization when the eye is not enough.

In early 2024, a finance employee in Hong Kong joined a video call with people who looked and sounded like the company's chief financial officer and other colleagues. According to Hong Kong police, all of them were deepfake re-creations. The employee sent about 200 million Hong Kong dollars, about 25.6 million US dollars, in 15 transfers. The company, Arup, confirmed that "fake voices and images were used".⁸

What to check in images and video

The Detect Fakes project at the MIT Media Lab suggests paying attention to eight areas:⁵

- **The face.** High-end manipulations are almost always facial transformations.
- **Eyes and eyebrows.** Do shadows appear where you would expect them?
- **Facial hair.** Do the mustache, sideburns or beard look real?
- **Blinking.** Does the person blink enough, or too much?
- **Cheeks and forehead.** Is the skin too smooth or too wrinkly? Does the age of the skin match the hair and eyes?
- **Glasses.** Is there glare, is there too much, and does its angle change when the person moves?
- **Moles.** Does the mole look real?
- **Lips.** Do the lip movements look natural?

The FBI adds further signs: distorted hands or feet, unrealistic teeth or eyes, indistinct faces, unrealistic glasses or jewelry, inaccurate shadows, watermarks, lag time, voice matching and unrealistic movements.¹

What to check in voice and calls

- The FBI recommends listening closely to tone and word choice, to tell a real call from someone close to you from an AI-cloned voice.¹
- According to the FBI, fraudsters create short audio clips in a relative's voice, in an apparent crisis, asking for immediate financial help or demanding a ransom.¹ A crisis and a sense of urgency are reasons to stop and verify.
- In video calls, the FBI documented cases where lip movements did not fully match the audio, and coughs or sneezes were heard without matching movement on screen.²

What to check in remote job interviews

- In 2022 the FBI reported an increase in complaints about deepfakes and stolen personal data used to apply for remote positions, mostly in IT and software. Some of the positions included access to customer data, financial data and corporate systems.²
- In those cases, pre-employment background checks found that the details some applicants gave belonged to another person.²
- In 2025 the FBI reported that North Korean IT workers used artificial intelligence and face-swapping during video job interviews. One recommendation: ask "soft" questions about specific details of location and education.³

The important caveat

- In a study published in iScience in 2021, participants could not reliably detect deepfakes, and neither raising awareness nor a financial incentive improved their accuracy. Participants tended to judge fake videos as authentic, and overestimated their own ability to detect them.⁶
- MIT stresses that there is no single tell-tale sign of a fake.⁵
- NIST notes a gap between the high accuracy of detection tools in research and the difficulty of using them in the real world.⁷

So a suspicious sign is a reason to check, but the absence of signs does not prove the content is real. The main protection is procedure, as set out on the next page.

PROCEDURES THAT DO NOT DEPEND ON THE EYE

An unusual instruction by phone or video

- The FBI recommends hanging up, looking up the phone number of the organization that claims to be calling, and calling it directly.¹
- The FBI recommends that families agree on a secret word or phrase to verify identity.¹ The same principle applies in an organization, between managers and the people who make payments. This is this document's adaptation, not an FBI recommendation for organizations.
- A transfer of money or sensitive information above a threshold set in advance should require approval from a second person, through a separate channel. In the Arup case, one employee made 15 transfers after a single video call.⁸

Hiring and remote workers

- The FBI recommends verifying identity during interviews, during onboarding and throughout employment.³
- The FBI recommends completing as much of the hiring and onboarding process as possible in person.³
- A background check cross-checks the details a candidate gave against independent sources. According to the FBI, such checks found that the details of some applicants belonged to another person.²

Senior staff and sensitive communications

- According to the NSA, the FBI and CISA, synthetic media threats include impersonating leaders and financial officers. They recommend considering real-time verification, and protecting senior officers and their communications.⁴
- The FBI recommends limiting images and voice recordings online, making social media accounts private and limiting followers to people you know. The less material is public, the harder it is to build a fake identity.¹

Preparation and response

- The NSA, the FBI and CISA recommend information sharing, planning and rehearsing responses to exploitation attempts, and personnel training.⁴

Before deciding on the basis of a video

A video that appears to show an employee, a manager or an event is not enough on its own. Before responding, check five questions:

- 1 **Source:** who published the video first, and when?
- 2 **Identity:** does the person in the video match their digital identity over time?
- 3 **Corroboration:** is there independent evidence of the claimed event?
- 4 **Activity patterns:** have new accounts or identity changes appeared recently?
- 5 **Context and motives:** who is behind the distribution, and are there signs of an attempt to deceive?

Open sources can also be fake, and the absence of findings does not prove that a person or a video is authentic.

The full article, with the video, in the Knowledge Hub: profcheck.co/knowledge/deepfake-lineup-insider-threat

Sources

1. FBI (IC3), Alert I-120324-PSA, 3 December 2024. ic3.gov/PSA/2024/PSA241203
2. FBI (IC3), Alert I-062822-PSA, 28 June 2022. ic3.gov/PSA/2022/PSA220628
3. FBI (IC3), Alert I-012325-PSA, 23 January 2025. ic3.gov/PSA/2025/PSA250123
4. NSA, FBI and CISA, Contextualizing Deepfake Threats to Organizations, 12 September 2023. nsa.gov/Press-Room/Press-Releases-Statements/Article/3523329
5. Detect Fakes project, MIT Media Lab. media.mit.edu/projects/detect-fakes/overview
6. Köbis, Doležalová & Soraperra, "Fooled twice: People cannot detect deepfakes but think they can", iScience 24(11), 2021. doi.org/10.1016/j.isci.2021.103364
7. NIST, Guardians of Forensic Evidence program. nist.gov/programs-projects/guardians-forensic-evidence
8. CNN on Arup, 16 May 2024. edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk